

---

# Contents

|  |             |
|--|-------------|
| <b>List of Figures and Tables</b>                | <b>ix</b>   |
| <b>Foreword</b>                                  | <b>xi</b>   |
| <b>Preface</b>                                   | <b>xv</b>   |
| <b>Acknowledgments</b>                           | <b>xvii</b> |
| <b>PART ONE THE CHALLENGE OF THE FRONTIER</b>    | <b>1</b>    |
| <b>Chapter 1: Living at the Digital Frontier</b> | <b>3</b>    |
| Increasing Complexity                            | 4           |
| The Digital Security Gap                         | 5           |
| Mapping the Digital Frontier                     | 6           |
| Step One: Assessing the Environment              | 7           |
| Step Two: Determining Responsibilities           | 10          |
| Step Three: Setting Priorities                   | 11          |
| Challenges at the Frontier                       | 13          |
| Threats and Vulnerabilities                      | 13          |
| An Attack Scenario                               | 15          |
| <b>Chapter 2: Security Characteristics</b>       | <b>21</b>   |
| Aligned  | 22          |
| Enterprise-Wide                                  | 26          |
| Continuous                                       | 28          |

---

|   |           |
|---|-----------|
| Proactive   | 30        |
| Validated   | 32        |
| Formal  | 35        |
| <b>Chapter 3: Organisational Components and Security Objectives</b> | <b>41</b> |
| Organisational Components   | 43        |
| People  | 43        |
| Process   | 44        |
| Technology  | 46        |
| Security Objectives   | 47        |
| Confidentiality, Integrity, and Availability                        | 47        |
| Access Control  | 48        |
| Segregation of Duties   | 51        |
| <b>PART TWO THE AGENDA FOR ACTION</b>                               | <b>55</b> |
| <b>Chapter 4: The Security Agenda</b>                               | <b>59</b> |
| Policies, Standards, and Guidelines                                 | 62        |
| Intrusion and Virus Detection                                       | 65        |
| Incident Response   | 69        |
| Active Attacks  | 70        |
| Passive Attacks   | 71        |
| Privacy   | 77        |
| Physical Security   | 81        |
| Asset and Service Management  | 84        |
| Vulnerability Management  | 87        |
| Vulnerabilities within Information Systems                          | 88        |
| Entitlement Management  | 91        |
| Business Continuity Planning  | 94        |
| Conclusion  | 98        |
| <b>Chapter 5: The Security Life Cycle</b>                           | <b>99</b> |
| Organisational Model  | 99        |
| Planning, Architecture, Operations, and Monitoring Capabilities     | 102       |
| Planning  | 104       |
| Architecture  | 110       |
| Operations  | 111       |
| Monitoring  | 113       |

---

|  |                                |            |
|--|--------------------------------|------------|
| <b>PART THREE</b>  | <b>THE APPROACH FOR SAFETY</b> | <b>117</b> |
| <b>Chapter 6: The Security Culture</b>                                   |                                | <b>119</b> |
| Sponsorship  |                                | 120        |
| The Chief Executive as an Agent of Change                                |                                | 121        |
| Instil a Heightened Sense of Awareness                                   |                                | 121        |
| Assign Ownership   |                                | 121        |
| Accountability   |                                | 122        |
| Build a Digital Security Guidance Council                                |                                | 122        |
| Establish a Timetable and Monitor Progress                               |                                | 123        |
| Roll Out an Enterprise-Wide Security Awareness<br>and Training Programme |                                | 124        |
| The Extended Security Culture  |                                | 126        |
| <b>Chapter 7: The Risk Frontier</b>                                      |                                | <b>129</b> |
| Modeling and Defining Digital Security Risk                              |                                | 130        |
| “Low and Slow” Scenario: Lessons to Be Learned                           |                                | 136        |
| High-Impact Risk Scenario: Lessons to Be Learned                         |                                | 140        |
| Containment and Control Scenarios:<br>Lessons to Be Learned              |                                | 142        |
| Approaching Risk Management  |                                | 143        |
| <b>Chapter 8: Road Map for Success</b>                                   |                                | <b>145</b> |
| Positioning the Organisation within the Industry                         |                                | 147        |
| Resource Allocation  |                                | 150        |
| Insuring against Digital Security Events                                 |                                | 152        |
| Table-Top Exercises  |                                | 153        |
| Executive Radar  |                                | 155        |
| <b>Appendix A: Security-Related Laws and Regulations</b>                 |                                | <b>159</b> |
| Balancing Competing Interests  |                                | 160        |
| Cross-Border Issues  |                                | 161        |
| Sources of Security-Related Laws and Regulations                         |                                | 161        |
| Data Security  |                                | 162        |
| Detection and Investigation of Crime<br>and National Security Matters    |                                | 164        |
| Fundamental Rights   |                                | 167        |
| Privacy  |                                | 167        |
| Free Speech  |                                | 168        |
| Property Rights  |                                | 169        |
| Conclusions  |                                | 170        |

---

|  |            |
|--|------------|
| Examples of National Security-Related Laws<br>and Regulations  | 170        |
| Australia  | 170        |
| Canada   | 171        |
| Denmark  | 171        |
| European Union   | 172        |
| India  | 172        |
| Malaysia   | 173        |
| Netherlands  | 173        |
| Poland   | 173        |
| Singapore  | 173        |
| South Africa   | 173        |
| United Kingdom   | 174        |
| United States  | 175        |
| <b>Appendix B: Threat Vectors</b>  | <b>179</b> |
| Outsourcing/Offshoring   | 179        |
| Cost Management  | 181        |
| Governance   | 182        |
| Terrorism  | 183        |
| New and Evolving Technologies  | 183        |
| Data Management  | 184        |
| Malware  | 184        |
| Mobile Working   | 185        |
| Mergers, Acquisitions, and Alliances   | 186        |
| Performance Management and Reporting   | 187        |
| <b>Appendix C: Ernst &amp; Young 2004 Digital Security<br/>    Overview: An Executive Guide and Diagnostic</b> | <b>189</b> |
| <b>Endnotes</b>  | <b>229</b> |
| <b>Glossary of Digital Security Terminology</b>  | <b>231</b> |
| <b>Index</b>   | <b>245</b> |